

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
GALVESTON DIVISION**

BEVERLY T. PETERS,
individually and on behalf of all
others similarly situated,

PLAINTIFF

v.

ST. JOSEPH SERVICES CORP.
d/b/a **ST. JOSEPH HEALTH**
SYSTEM and
ST. JOSEPH REGIONAL HEALTH
CENTER,

DEFENDANTS

CASE NO.: 3:14-cv-00114

JURY TRIAL DEMANDED

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Beverly T. Peters (“Peters” or “Plaintiff”), on behalf of herself and all others similarly situated, brings this action against Defendants St. Joseph Services Corporation d/b/a St. Joseph Health System and St. Joseph Regional Health Center (together, “St. Joseph” or “Defendants”), and respectfully shows the following:

NATURE OF THE CASE

1. This is a consumer class action data breach lawsuit involving the unauthorized disclosure of personally identifiable information (“PII”) and protected health information (“PHI”) (together, “PII/PHI”). Plaintiff brings

this action, individually and on behalf of approximately 405,000 similarly situated persons (*i.e.*, the Class Members), who entrusted their PII/PHI to St. Joseph in connection with purchasing health care services from St. Joseph based on St. Joseph's assurances that the proper data security measures, policies, procedures and protocols were in place and operational to safeguard and protect their PII/PHI.

2. St. Joseph, however, willfully, intentionally, recklessly and/or negligently failed to safeguard and protect Plaintiff's and Class Members' PII/PHI, which was accessed, stolen and disseminated into the public domain by a thief or thieves from St. Joseph's inadequately protected computer system (the "Data Breach"). On information and belief, the stolen and compromised PII/PHI was unencrypted. The St. Joseph Data Breach is one of the largest data breaches involving stolen and compromised PHI in the history of the United States.

3. Plaintiff is a former St. Joseph patient. The Class Members are current and former St. Joseph patients, employees and some employees' beneficiaries. According to St. Joseph's February 4, 2014 press release revealing the Data Breach, the stolen and compromised PII/PHI include names, Social Security numbers, dates of birth, medical information (*i.e.*, PHI), and possibly addresses. The Data Breach also could involve other forms of Plaintiff's and Class Members' PII/PHI. The investigation is ongoing.

4. St. Joseph flagrantly disregarded Plaintiff's and Class Members' privacy rights by intentionally, willfully, recklessly and/or negligently failing to take the necessary precautions required to safeguard and protect their PII/PHI from unauthorized disclosure. Plaintiff's and Class Members' PII/PHI was improperly handled and stored by St. Joseph, inadequately secured, on information and belief, unencrypted, and not kept in accordance with applicable, required, and appropriate cyber-security measures, policies, procedures and/or protocols. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, Plaintiff's and Class Members' PII/PHI was stolen and compromised, and Plaintiff has suffered identity theft, identity fraud and/or medical fraud.

5. By its wrongful actions, inaction and/or omissions and the resulting Data Breach, St. Joseph willfully and recklessly or, at the very least, negligently, violated the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA"). St. Joseph failed to safeguard and protect Plaintiff's and Class Members' PII/PHI, which is specifically protected by FCRA, by failing to limit its dissemination for permissible purposes authorized by FCRA. As a direct and/or proximate result of St. Joseph willful, reckless and/or grossly negligent FCRA violations, unauthorized third parties, operating from IP addresses in China and elsewhere, obtained Plaintiff's and Class Members' PII/PHI for no permissible purpose under FCRA.

6. St. Joseph's wrongful actions, inaction and/or omissions and the resulting Data Breach also violated the Texas Medical Practice Act, TEX. OCC. CODE § 159.001, *et seq.*, the Texas Hospital Licensing Law, TEX. HEALTH & SAFETY CODE § 241.001, *et seq.*, and the Texas Deceptive Trade Practices-Consumer Protection Act, TEX. BUS. & COM. CODE § 17.41, *et seq.*

7. St. Joseph's wrongful actions, inaction and/or omissions and the resulting Data Breach also constitute negligence/gross negligence, negligence *per se*, breach of contract, breach of implied contract, invasion of privacy, breach of fiduciary duty, breach of confidentiality, and money had and received/assumpsit under Texas common law.

8. Plaintiff, on behalf of herself and the Class Members, seeks actual damages, consequential damages, statutory damages, nominal damages, exemplary damages, treble damages, injunctive relief, attorneys' fees, litigation expenses and/or costs of suit.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over Plaintiff's FCRA claims pursuant to 28 U.S.C. § 1331 (federal question). This Court also has subject matter jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367. This Court has personal jurisdiction over St. Joseph because at all relevant times, St. Joseph's headquarters were (and continue to be) in the Southern District

of Texas, and St. Joseph conducted (and continues to conduct) substantial business in the Southern District of Texas.

10. Venue is proper in the Galveston Division of the Southern District of Texas, pursuant to 28 U.S.C. § 1391(b) and (c), because at all relevant times, a substantial part, if not all, of the events giving rise to this action occurred in the Southern District of Texas, and St. Joseph resides, is located, can be found, and conducts substantial business in the Southern District of Texas. The federal venue statute for non-diversity cases, 28 U.S.C. § 1391, refers to venue in terms of districts, not divisions. Under federal law, there is no requirement that venue be laid in a particular division. Thus, since venue is proper in the Southern District of Texas, venue is proper in the Galveston Division of the Southern District of Texas. *See, e.g., U.S. v. Real Property Known as 200 Acres of Land Near Farm to Market Road 2686 in Rio Grande City, Texas*, No. 2:11-cv-00368, 2012 WL 1911270, at *2 (S.D. Tex. May 24, 2012) (citing *Says v. M/V David C. Devall*, 161 F.Supp.2d 752, 753 (S.D. Tex. 2001)). Moreover, pursuant to the June 5, 2014 Notice of Designation (Doc. #8), this Court specifically retained this case.

PARTIES

11. Plaintiff Peters is a citizen and resident of Brenham, Texas. Peters is a former St. Joseph patient who, at all relevant times, purchased and received health care services from St. Joseph and its affiliated physicians at several of its

health care facilities. Peters entrusted her PII/PHI to St. Joseph in connection with purchasing and receiving such health care services based on St. Joseph's assurances that the proper data security measures, policies, procedures and protocols were in place and operational to safeguard and protect her PII/PHI. Peters' PII/PHI, however, was stolen and compromised in the Data Breach—as confirmed by the February 4, 2014 Data Breach notification letter she received from St. Joseph. *See* Exhibit A.

12. Peters has never been victimized by a data breach other than the St. Joseph Data Breach. She meticulously protects her PII/PHI. She utilizes different passwords for each of her online financial, credit card, and retail accounts, changing them on a regular basis. She closely monitors her bank account, regularly checking it online at least every other day for irregular activity. She also maintains her hard copy credit card and financial account statements in a safe for five years, after which she personally burns them in a trash barrel on her property.

13. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions and the resulting Data Breach, Peters' PII/PHI was accessed and utilized by one or more unauthorized third parties who inflicted identity theft and/or identity fraud on her in the form of, *inter alia*, attempted unauthorized charges on her Discover card. Peters provided her Discover card account number to St. Joseph on forms she submitted to St. Joseph in connection

with purchasing health care services. After the Data Breach, and while she was in Texas, Peters received a text from Discover requesting approval of an unauthorized, out of the ordinary retail purchase in Pennsylvania. When Peters declined to approve the purchase, Discover immediately closed her account, and reissued a new payment card to her. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Discover card account.

14. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized access and utilization of her PII/PHI by one or more unauthorized third parties, Peters also suffered identity theft and/or identity fraud in the form of the breach of her Yahoo email account which, along with her Social Security number and Texas Driver's License number, was also submitted to St. Joseph in connection with purchasing health care services. All of Peters' online financial, credit card, and retail accounts are linked to her Yahoo email account. After the Data Breach, friends and relatives reported receiving large volumes of spam email from her Yahoo email account that they had never received before. As a result of this fraudulent activity, Peters changed the password on her Yahoo email account. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Yahoo email account and/or her online financial, credit card, and retail accounts.

15. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized access and utilization of her PII/PHI by one or more unauthorized third parties, Peters also suffered identity theft and/or identity fraud in the form of the unauthorized access of her Amazon.com account by an unidentified fraudster. Thereafter, another fraudster attempted to access her Amazon.com account using her son's name, which only could have been obtained from her stolen and compromised PHI wherein St. Joseph required her to provide the names and contact information of her next of kin. Peters' son confirmed he did not attempt to access her Amazon.com account. Prior to the Data Breach, Peters never experienced any attempt by fraudsters to access her Amazon.com account.

16. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized access and utilization of her PII/PHI by one or more unauthorized third parties, Peters also suffered identity theft, identity fraud and/or medical fraud in the form of multiple telephone solicitations from medical products and services companies asking to speak with specific members of her family. This information only could have been obtained from her stolen and compromised PHI wherein St. Joseph required her to provide the names and contact information of her next of kin. On the average,

Peters receives 2-3 such calls a day at all times of the day and night. Prior to the Data Breach, Peters never received such telephone solicitations.

17. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the unauthorized access and utilization of her PII/PHI by one or more unauthorized third parties, Peters also suffered identity theft, identity fraud and/or medical fraud in the form of unsolicited emailed and mailed marketing materials specifically targeting her confidential medical conditions listed in her stolen PII/PHI that the senders only could have learned by obtaining her stolen PII/PHI from the data thieves. Prior to the Data Breach, Peters never received such targeted marketing materials.

18. As a direct and/or proximate result of St. Joseph's wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft, identity fraud and/or medical fraud inflicted on her by one or more unauthorized third parties, Peters has suffered (and will continue to suffer) economic damages and other actual harm in the form of the deprivation of the value of her PII/PHI, for which there is a well-established national and international market. PII/PHI is a valuable property right.¹ Faced with the choice

¹ See, e.g., John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted). It is so valuable to

of having her PII/PHI stolen, compromised, bought, sold and utilized without authorization and receiving compensation versus selling her PII/PHI on the black market and receiving the compensation herself, Peters would choose the latter.²

identity thieves that once PII has been compromised, criminals often trade it on the “cyber black-market” for several years.

Theft of PHI is also gravely serious; to wit, “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.” See Federal Trade Commission, *Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited March 27, 2014). Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use stolen PHI to adjust their insureds’ medical insurance premiums.

The value of PHI as a commodity also is measurable. See, e.g., Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market* (April 28, 2014), <http://www.medscape.com/viewarticle/824192> (last visited June 26, 2014); Adam Greenberg, *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013) (all-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers and bank account information, complete with account and routing numbers, are fetching \$1,200 to \$1,300 each), <http://www.scmagazine.com/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/article/303302/> (last visited June 26, 2014).

² It also is important to note that in the case of identity theft or identity fraud, after a victim goes through the hassle of closing credit cards, changing passwords on financial accounts, and notifying lenders and the credit bureaus, the victim’s PII is again private from that point forward.

Peters—not data thieves—should have the exclusive right to monetize her PII/PHI at the highest values possible. St. Joseph’s wrongful actions, inaction and/or omissions and the resulting Data Breach deprived her of this right.

19. As a direct and/or proximate result of St. Joseph’s wrongful actions, inaction and/or omissions, the resulting Data Breach, and the resulting identity theft, identity fraud and/or medical fraud inflicted on her by one or more unauthorized third parties, Peters has suffered (and will continue to suffer) other economic damages and actual harm, including (i) invasion of privacy, (ii) the breach of her confidentiality by the improper disclosure of her PII/PHI without authorization, (iii) statutory damages under FCRA, (iv) lost benefit of her bargain, (v) diminished value of the medical services she purchased from St. Joseph, and

In the case of medical data breach, however, there is no opportunity for a clean start. Once a victim’s PHI is out—such as Peters’ and Class Members’ PHI—it is out forever. If there is a negative stigma associated with a victim’s PHI—such as a sexually-transmitted disease, an abortion, a sex change operation or a slow-growing cancer—it cannot be undone.

Even worse, the consequences of having one’s PHI fall into the hands of unscrupulous individuals can literally be life threatening. When a thief uses a victim’s PHI to obtain medical care, the imposter’s information could end up on the victim’s medical record. If the PHI theft victim subsequently was involved in an accident and rushed to the emergency room, doctors utilizing his or her PHI could see the wrong blood type, not know the victim is allergic to certain medications, and/or has a pre-existing condition—which, in turn, could lead to misdiagnosis or mistreatment with potentially deadly consequences.

(viii) emotional distress from the compromise of her PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date.

20. Defendant St. Joseph Services Corporation d/b/a St. Joseph Health System (“SJSC”) is a Texas corporation with its principal place of business in Bryan, Texas. SJSC is a health system originally established by the Sisters of St. Francis of Sylvania, Ohio, with five hospitals, two long term care centers, and over a dozen physician clinic locations serving more than 325,000 residents in eight Texas counties. SJSC already has been served with Summons, filed an Answer, and appeared in this action.

21. Defendant St. Joseph Regional Health Center (“SJRHC”) is a Texas corporation with its principal place of business in Bryan, Texas. SJRHC owns and operates a 310-bed regional health care center in Bryan, Texas, the anchor facility for SJSC, as well as several other St. Joseph health care facilities. Plaintiff purchased and received health care services from at least two of these St. Joseph facilities (and possibly also from SJSC). SJRHC already has been served with Summons, filed an Answer, and appeared in this action.

22. SJSC and SJRHC together will be referred to as “St. Joseph.”

23. At all relevant times, St. Joseph received, evaluated, assembled, transmitted, used and/or disclosed Plaintiff’s and Class Members’ PII/PHI in numerous ways (and continues to do so), including, *inter alia*: (i) in connection

with providing health care services to its patients, (ii) in connection with obtaining payment from insurance companies and state and federal government agencies, and via third-party collection agencies, (iii) for its own account in connection with its health care operations, including employment matters, and (iv) several other authorized purposes. *See* St. Joseph Notice of Privacy Practices (“Privacy Notice”) (Exhibit B). In doing so, St. Joseph received, evaluated, assembled, transmitted, used and/or disclosed Plaintiff’s and Class Members’ PII/PHI to insurance companies, state and federal government agencies, and/or third-party collection agencies for purposes of, *inter alia*, determining whether Plaintiff and Class Members were (and are) eligible for various health care services, determining whether such health care services were (and are) covered by health insurance, and obtaining payment for such health care services. The insurance companies, state and federal government agencies, and third-party collection agencies, in turn, utilize Plaintiff’s and Class Members’ PII/PHI for a variety of purposes, including, *inter alia*, setting rates for health insurance, life insurance, and other types of insurance, setting rates for the payment of future health care services, evaluating insurance coverage issues and/or collecting for and/or paying St. Joseph for providing health care services.

BACKGROUND FACTS

I. Data breaches lead to identity theft, identity fraud and/or medical fraud, and multiple forms of economic damages and other actual harm.

24. According to the United States Government Accountability Office (GAO), the terms “identity theft” or “identity fraud” are broad terms encompassing various types of criminal activities, such as credit card fraud, telephone or utilities fraud, bank fraud and government fraud (*i.e.*, theft of government services). Identity theft occurs when a person’s PII/PHI is used without authorization to commit fraud or other crimes. *See* Federal Trade Commission, *Fighting Back against Identity Theft*.³ According to the FTC:

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

Id.

25. Also according to the FTC, “the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from

³ <http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html> (last visited March 27, 2014).

unanticipated uses of data.”⁴ Furthermore, “there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII.”⁵

26. Moreover, “[o]nce identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax refund in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.”⁶

27. Medical fraud (also known as medical identity theft) occurs when a person’s personal information is used without authorization to obtain, or receive

⁴ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012), <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (last visited June 26, 2014).

⁵ Federal Trade Commission, *A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, (Dec. 2010), <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf> (last visited June 26, 2014).

⁶ Federal Trade Commission, *Signs of Identity Theft*, <http://www.consumer.ftc.gov/articles/0271-signs-identity-theft> (last visited March 27, 2014).

payment for, medical treatment, services or goods.⁷ For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. “Victims of medical identity theft [also] may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.” *Id.*⁸

28. A fraudster can easily research the email address of a data breach victim. When a fraudster has access to PII/PHI from a large group of similarly situated victims, it is much more feasible to develop a believable phishing⁹ spoof email that appears realistic. The fraudsters can then convince the group of victims to reveal additional private financial account and payment card information.

⁷ www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html (last visited March 24, 2014).

⁸ *See* www.ftc.gov/bcp/edu/microsites/idtheft/consumers/resolving-specific-id-theft-problems.html (last visited March 27, 2014).

⁹ “Phishing” is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and often directs users to enter details at a fake website that looks and feels almost identical to the legitimate one.

29. The GAO found that identity thieves use PII/PHI to open financial and payment card accounts, and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take a while for the victim to become aware of the theft. In the meantime, the identity theft causes significant harm to the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security numbers are incredibly difficult to change and their misuse can continue for years into the future.

30. Identity thieves also use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes and/or filing fraudulent tax returns on the victim's behalf to obtain fraudulent tax refunds. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in the victim's name. Identity thieves also have been known to give a victim's personal information to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

31. The unauthorized disclosure of a person's Social Security number can be particularly harmful since Social Security numbers cannot be easily replaced

like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone used the number fraudulently and the victim is being disadvantaged by the misuse.¹⁰ Thus, a PII/PHI theft victim cannot obtain a new Social Security number until the damage has already been done.

32. Obtaining a new Social Security number also is not an absolute prevention against identity theft and identity fraud. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft and identity fraud, a new number may actually create new problems. Because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history. Thus, data breaches lead to identity theft, identity fraud and/or medical fraud, and multiple forms of economic damages and other actual harm.

II. The Privacy Notice—St. Joseph's Contractual Privacy Obligations to its Patients.

33. As a condition to providing health care services, St. Joseph requires its patients to provide their detailed PII/PHI. Indeed, St. Joseph recognizes that maintaining the confidentiality of its patients' PII/PHI is critical:

¹⁰ See *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (October 2007), <http://www.ssa.gov/pubs/10064.html> (last visited June 26, 2014).

Safeguarding patients' health information is *not only a legal requirement but also an important ethical obligation*. As a health care provider, St. Joseph and its staff are entrusted with clinical information regarding our patients. *We recognize that medical and billing records are highly confidential and must be treated with great respect and care* by all staff with access to this information. St. Joseph's policy regarding confidentiality of protected health care information reflects *our strong commitment to protecting the confidentiality of our patients' medical records and clinical information*.¹¹

(emphasis added).

34. St. Joseph makes certain representations, warranties and commitments to its patients regarding the privacy of their PII/PHI in its Privacy Notice (Exhibit B). The Privacy Notice is posted in each St. Joseph facility (*id.* at 1) and on the St. Joseph website.¹² The Privacy Notice is also given to every St. Joseph patient—including Plaintiff and Class Members. Indeed, each St. Joseph patient must sign the Privacy Notice, acknowledging its existence and terms as a condition to receiving health care services. *Id.* at 3. Plaintiff signed the Privacy Notice.

35. St. Joseph itemizes its privacy obligations to its patients in the Privacy Notice, making a firm commitment to uphold them; to wit, “St. Joseph is required

¹¹ See <http://www.st-joseph.org/body.cfm?id=461> (last visited March 25, 2014).

¹² See <http://www.st-joseph.org/workfiles/privacy.pdf> (last visited March 22, 2014).

by law¹³ to maintain the privacy of health information about you that can identify you ('Protected Health Information' or 'PHI'), to provide you with this Notice of our legal duties and privacy practices with respect to your PHI, and to abide by the terms of the Notice currently in effect.” *Id.* at 1. St. Joseph further pledges:

We understand that all information about you and your health is personal. We are committed to protecting this information. When you receive services at a St. Joseph Facility/Entity, a medical record is created. This record describes the services provided to you and is needed to provide you with quality care and to comply with certain legal requirements. This Notice applies to records of your care generated by St. Joseph, whether made by a St. Joseph employee or a physician involved in your care.

Id. at 1 (emphasis added).

36. The Privacy Notice lists the following specific and limited permissible purposes for which St. Joseph may use and disclose all or a portion of its patients' PII/PHI without their authorization:

- (i) Treatment, payment and health care operations;
- (ii) Sharing with other organizations in connection with treatment, payment and health care operations;
- (iii) Inclusion in a specific St. Joseph facility patient directory;

¹³ See, e.g., Health Insurance Portability and Accountability Act of 1996, as amended, 42 U.S.C. § 1320d, *et seq.* (“HIPAA”), Texas Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE § 181.001, *et seq.*, Texas Medical Practice Act, TEX. OCC. CODE § 159.001, *et seq.*, Texas Hospital Licensing Law, TEX. HEALTH & SAFETY CODE § 241.001, *et seq.*, and TEX. BUS. & COM. CODE §§ 521.052; 521.053.

- (iv) Disclosure to relatives and close friends to the extent necessary to assist with a patient's health care or to secure payment for the patient's health care;
- (v) Disclosure for purpose of assisting disaster relief efforts;
- (vi) Medical research in limited situations;
- (vii) Fundraising activities; and
- (viii) Disclosures required by law, such as pertaining to various listed public health activities.

Id. at 1-2.

37. *"For any purpose other than the ones described above, your PHI may be used or disclosed only when you provide your written authorization on an approved authorization form."* Privacy Notice at 2 (emphasis added). In other words, St. Joseph commits that *"for any purpose other than the ones described above,"* a patient's PII/PHI will not be disclosed without authorization. *Id.* There are no exceptions.

38. Regarding its patients' rights pertaining to their PHI, St. Joseph further represents and promises that "[i]n certain [undefined] instances, you have the right to be notified in the event that we, or one of our Business Associates, discover an inappropriate use or disclosure of your health information. Notice of any such use or disclosure will be made in accordance with state and federal requirements." Privacy Notice at 3.

39. St. Joseph further represents and promises its patients that they also “have the right to request an ‘accounting of disclosures.’ This is a list of disclosures that we have made about you.” *Id.*

40. Finally, regarding the PII/PHI entrusted to it, St. Joseph represents and promises that it “safeguards customer information using various tools such as firewalls, passwords and data encryption” and “continually strive[s] to improve these tools to meet or exceed industry standards.” *Id.* Ironically, St. Joseph also promises to “limit access to [its patients’] information to protect against its unauthorized use.” *Id.* St. Joseph’s data security efforts, however, unfortunately failed across the board.

III. The St. Joseph Data Breach.

41. On February 4, 2014, St. Joseph announced to the public, for the first time, that between December 16, 2013 and December 18, 2013, a server on its computer system storing patient and employee files for several St. Joseph facilities (*i.e.*, their PII/PHI) granted unauthorized access to parties operating from IP addresses in China and elsewhere.

42. The infiltrated server contained the PII/PHI of Plaintiff and approximately 405,000 Class Members, which was stolen, compromised and disseminated into the public domain (the “Data Breach”). The stolen and compromised PII/PHI includes names, Social Security numbers, birthdates,

addresses, medical information, and bank account information. Other information may also have been stolen. On information and belief, none of the stolen and compromised PII/PHI was encrypted. The Data Breach is one of the largest medical data breaches in the history of the United States.

43. St. Joseph also announced it was belatedly “taking appropriate additional security measures to strengthen the security of its system,” (*id.*), which are the PII/PHI data security measures, policies, procedures, protocols, and software and hardware systems it should already have instituted. Had such PII/PHI data security measures, policies, procedures, protocols, and software and hardware systems been in place, functioning and properly monitored, the Data Breach never would have occurred. On information and belief, at the time of the Data Breach, St. Joseph was not compliant with HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Section 521.052 of the Texas Business and Commerce Code, and/or the industry standards it references in its Privacy Notice that St. Joseph claims to “meet or exceed.” *See* Privacy Notice (Exhibit B) at 3.

44. What’s more, despite knowing about the Data Breach since at least December 18, 2013, St. Joseph did not announce the Data Breach and/or commence sending Data Breach notification letters to Plaintiff and Class Members until February 4, 2014—almost seven weeks later. St. Joseph’s failure to timely

notify Plaintiff and Class members about the Data Breach notification violated Section 521.053 of the Texas Business and Commerce Code. Had Plaintiff and Class Members known about the Data Breach sooner, they could have taken certain defensive measures much earlier—such as changing financial account and payment card passwords and email addresses—to mitigate their injuries and damages. St. Joseph’s Data Breach notification delay, therefore, also substantially increased the risk of additional real and impending future economic damages and other actual harm to Plaintiff and Class Members resulting from identity theft, identity fraud and/or medical fraud.

45. During the intervening period between the Data Breach and the date the Data Breach notification letters were sent to Plaintiff and Class Members, their unencrypted PII/PHI, on information and belief, was bought and sold several times on the robust international cyber black market—as evidenced by the identity theft, identity fraud and/or medical fraud Plaintiff has already suffered—while they had no chance whatsoever to take measures to protect the its confidentiality.

46. Rather than getting out in front of the Data Breach and proactively offering Plaintiff and Class Members real protection from identity theft, identity fraud and/or medical fraud resulting from their stolen and compromised PII/PHI, St. Joseph only offered Plaintiff and Class Members one year of credit monitoring (Exhibit A)—even though it is well known that data thieves routinely use stolen

PII/PHI for longer than a year, and sometimes wait more than a year to use stolen information until the conclusion of one year basic credit monitoring programs breached organizations typically offer. Even then, only a year of credit monitoring is woefully insufficient given the trove of unencrypted PII/PHI stolen and disseminated to the world in the St. Joseph Data Breach and the manipulation and machinations of cyber criminals.

47. In truth, the actual post-Data Breach “PII/PHI protection services” allegedly offered by St. Joseph and at what price are remarkably indiscernible—which could be a violation of the Texas Deceptive Trade Practices-Consumer Protection Act in itself. At best, the proffered credit monitoring indirectly tracks identity theft; while it may reveal new credit accounts opened with the stolen information, it will do nothing to monitor unauthorized charges made to, for example, existing payment card accounts. After data breach victims enroll in this type of program, program vendors and the credit reporting agencies typically treat their enrollment as golden opportunities to push other unnecessary products and services—thereby further damaging data breach victims.

48. Notwithstanding St. Joseph’s promises, the offered “PII/PHI protection services,” in truth, are significantly less than advertised. In the fine print in its Terms of Use attached to the St. Joseph Data Breach notification letters (Exhibit A), AllClear ID, the credit monitoring program vendor, states it (i) “will

not make payments or reimbursements to you for any loss or liability you may incur,” and (ii) “does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.” As a further condition of receiving AllClear ID “protection services,” Plaintiff and Class Members must not fall victim to phishing emails and disclose their PII—which could easily result from the Data Breach. In other words, if a Class Member is victimized by a phishing scam fueled by the PII/PHI disclosed by St. Joseph in the Data Breach, he or she will lose the AllClear ID “protection services” offered as a result of the Data Breach.

49. St. Joseph’s Data Breach notification letters also are a less-than-subtle attempt to shift the burden and expense of the Data Breach to Plaintiff and Class Members by, *inter alia*, advising and encouraging them to incur the time and expense to (i) regularly purchase their credit reports from the three major credit reporting agencies, (ii) contact the agencies, law enforcement, state attorney general and/or the FTC if anything in their financial or retail accounts look amiss, (iii) place fraud alerts on their credit reports, and (iv) place and/or lift freezes on their credit files, which must be instituted at each credit reporting agency (*i.e.*, Equifax, Experian, and TransUnion) at a cost of \$5 to \$20 an action. All of these actions will take time and money to effectuate—which St. Joseph has advised and encouraged Plaintiff and Class Members to incur, but not offered to pay.

IV. The St. Joseph Data Breach Inflicted Economic Damages and Other Actual Harm on Plaintiff and Class Members.

50. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, failing to protect Plaintiff's and Class Members' PII/PHI with which it was entrusted—directly and/or proximately caused the Data Breach, theft and dissemination of Plaintiff's and Class Members' unencrypted PII/PHI into the public domain without their knowledge, authorization, and/or consent.

51. St. Joseph flagrantly and/or negligently disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by not obtaining their prior written consent to disclose their PII/PHI to any other person or organization and/or for any purpose other than the persons, organizations and purposes listed in the Privacy Notice—as required by, *inter alia*, the Privacy Notice, FCRA, HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Section 521.052 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that St. Joseph claims to “meet or exceed.” *See* Exhibit B at 3.

52. St. Joseph flagrantly and/or negligently disregarded and/or violated Plaintiff's and Class Members' privacy rights, and harmed them in the process, by failing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI.

St. Joseph's unwillingness or inability to identify, implement, maintain and/or monitor such data security measures, policies procedures, protocols, and software and hardware system—while, at the same time, claiming in its Privacy Notice that such “tools” were in place (*id.* at 3)—is an abuse of discretion, false, and misleading, confirming St. Joseph's intentional and willful conduct.

53. St. Joseph's untimely and inadequate Data Breach notification—including its failure to provide Plaintiff and Class Members with any meaningful protection or relief from the Data Breach—is misleading and, even worse, substantially increases Plaintiff's and Class Members' risk of long term future economic damages and other actual harm resulting from identity theft, identity fraud and/or medical fraud.

54. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, and caused Plaintiff and Class Members to suffer economic damages and other actual harm. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members'

PII/PHI would not have been stolen, compromised, disseminated to the world and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under FCRA, (v) lost benefit of their bargains, (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vii) diminished value of the medical services they purchased from St. Joseph, and (viii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date.

CLASS ACTION ALLEGATIONS

55. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a class action on behalf of herself and the following Class of similarly situated individuals:

All Texas residents who were sent a letter or other communication by St. Joseph notifying them that their personally identifiable information and/or protected health information was maintained on a St. Joseph Health System computer system server that was breached by hackers between December 16, 2013 and December 18, 2013, inclusive.

Excluded from the Class are (i) St. Joseph officers and directors, and (ii) the Court, Court personnel, and members of their immediate families.

56. The Class Members are so numerous that their joinder is impracticable. According to information provided by St. Joseph, there are over 400,000 Class Members. The precise identities of the Class Members and their addresses are currently unknown to Plaintiff, but can be easily derived from St. Joseph's internal records that were used to send the Data Breach notification letters to Plaintiff and Class Members in early February 2014.

57. St. Joseph's above-described wrongful actions, inaction and/or omissions that caused the Data Breach and the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI violated the rights of Plaintiff and each Class Member in a virtually identical manner.

58. Questions of law and fact common to all Class Members predominate over any questions affecting only individual Class Members including, *inter alia*:

- (i) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI willfully or negligently violated FCRA;
- (ii) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI violated the Texas Medical Practice Act;
- (iii) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI violated the Texas Hospital Licensing Law;
- (iv) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes negligence and/or gross negligence;
- (v) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes negligence *per se*;

- (vi) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes breach of contract;
- (vii) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes breach of implied contract;
- (viii) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI violated the Texas Deceptive Trade Practices-Consumer Protection Act;
- (ix) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes invasion of privacy.
- (x) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes breach of fiduciary duty;
- (xi) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI constitutes a breach of confidentiality at Texas common law;
- (xii) Whether St. Joseph's failure to safeguard and protect Plaintiff's and Class Members' PII/PHI invokes the equitable doctrines of money had and received/assumpsit;
- (xiii) Whether Plaintiff and Class Members sustained harm and damages as a direct and/or proximate result of St. Joseph's failure to safeguard and protect their PII/PHI and, if so, the amount of such damages;
- (xiv) Whether Plaintiff and Class Members are entitled to exemplary damages as a direct and/or proximate result of St. Joseph's failure to safeguard and protect their PII/PHI and, if so, the amount of such damages; and
- (xv) Whether Plaintiff and Class Members are entitled to injunctive relief as a direct and/or proximate result of St. Joseph's failure to safeguard and protect their PII/PHI.

59. Plaintiff's claims are typical of the Class Members' claims because Plaintiff, like all Class Members, is a victim of St. Joseph's above-described

wrongful actions, inaction and/or omissions—to wit, St. Joseph’s failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ PII/PHI—that directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff’s and Class Members’ PII/PHI, and caused Plaintiff and Class Members to suffer the resulting economic damages and other actual harm.

60. Plaintiff and her counsel will fairly and adequately represent the Class Members’ interests. Plaintiff has no interests antagonistic to, or in conflict with, Class Members’ interests. Plaintiff is willing and able to take an active role in controlling the litigation and protecting the absent class members. Plaintiff’s attorneys are highly experienced in the prosecution of consumer class actions and data breach class actions, and intend to vigorously prosecute this action on behalf of Plaintiff and Class Members as they have to date.

61. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff’s and Class Members’ claims. Plaintiff and Class Members have been irreparably harmed as a result of St. Joseph’s wrongful actions, inaction and/or omissions and the resulting Data Breach. Litigating this case as a class action is appropriate because (i) it will avoid a multiplicity of suits and the corresponding burden on the courts and Parties, (ii) it would be virtually

impossible for all Class Members to intervene as parties-plaintiff in this action, (iii) it will allow numerous individuals with claims too small to adjudicate on an individual basis because of prohibitive litigation costs to obtain redress for their injuries, and (iv) it will provide Court oversight of the claims process once St. Joseph's liability is adjudicated.

62. Class certification, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

63. Class certification also is appropriate under FED. R. CIV. P. 23(b)(2) because St. Joseph has acted or refused to act on grounds generally applicable to the Class, thereby making final injunctive relief appropriate with respect to the Class as a whole.

64. Class certification also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for St. Joseph. For example, one court might decide that the challenged actions are illegal and enjoin St. Joseph while another court might decide the same actions, inaction and/or omissions are not illegal. Individual actions also could be dispositive of, impair or impede the interests of Class Members who are not parties to such actions.

65. Absent a class action, St. Joseph will escape liability for its wrongdoing despite its serious violations of the law and the infliction of economic damages and other actual harm on Plaintiff and Class Members.

CLAIMS FOR RELIEF/CAUSES OF ACTION

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT (15 U.S.C. § 1681, *et seq.*)

66. The preceding factual statements and allegations are incorporated by reference

67. In enacting FCRA, Congress made several findings, including that consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit information and other consumer information—such as PII/PHI (15 U.S.C. § 1681(a)(3))—and “[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and *a respect for the consumer's right to privacy.*” 15 U.S.C. § 1681(a)(4) (emphasis added).

68. Under 15 U.S.C. § 1681a(f), a “consumer reporting agency” includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing

“consumer reports” to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

69. Under 15 U.S.C. § 1681a(d)(1), a “consumer report” is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b.

70. “Consumer credit information” (PII) includes, *inter alia*, a person's name, identification number (*e.g.*, Social Security number), marital status, physical address and contact information, educational background, employment, professional or business history, financial accounts and financial account history (*i.e.*, details of the management of the accounts), credit report inquiries (*i.e.*, whenever consumer credit information is requested from a credit reporting agency), judgments, administration orders, defaults, and other notices.

71. Under 15 U.S.C. § 1681a(i), “medical information” (PHI) is information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to the (i) past,

present, or future physical, mental, or behavioral health or condition of an individual, (ii) provision of health care to an individual, and (iii) payment for the provision of health care to an individual.

72. FCRA limits the dissemination of “consumer credit information” (PII) to certain well-defined circumstances and no other. 15 U.S.C. § 1681b(a). FCRA also specifically protects “medical information” (PHI). *See, e.g.*, 15 U.S.C. §§ 1681a(d)(3) (“Restriction on sharing of medical information”); 1681b(g) (“protection of medical information”); 1681c(a)(6) (“Information excluded from consumer reports”).

73. At all relevant times, Plaintiff and Class Members were consumers of health care services from St. Joseph and its employed and/or affiliated health care professionals. As such, Plaintiff’s and Class Members’ PII/PHI, which was delivered to St. Joseph in connection with purchasing such health care services based on St. Joseph’s commitment to safeguard and protect the PII/PHI, in whole or in part, is “consumer credit information” and/or “medical information” protected by FCRA.

74. At all relevant times, St. Joseph was (and continues to be) a consumer reporting agency under FCRA because on a cooperative nonprofit basis and/or for monetary fees, St. Joseph regularly (i) received, assembled and/or evaluated Plaintiff’s and Class Members’ “consumer credit information” and/or “medical

information” protected by FCRA (*i.e.*, their PII/PHI) for the purpose of furnishing consumer reports to third parties, and (ii) used the means and/or facilities of interstate commerce to prepare, furnish and transmit consumer reports containing Plaintiff’s and Class Members’ PII/PHI to third parties—for the ultimate purposes of, *inter alia*, establishing Plaintiff’s and Class Members’ eligibility for health care services, confirming whether such health care services were covered by their health insurance and/or securing payment for the provision of such health care services (and continues to do so).

75. As a consumer reporting agency, St. Joseph was (and continues to be) required to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard, protect and limit the dissemination of consumer credit information and medical information in its possession, custody and control, including Plaintiff’s and Class Members’ PII/PHI, only for permissible purposes under FCRA. *See* 15 U.S.C. § 1681(b).

76. By its above-described wrongful actions, inaction and/or omissions, however, St. Joseph willfully and/or recklessly violated FCRA; to wit, St. Joseph willfully and/or recklessly violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and/or 15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the

proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI which, in turn, directly and/or proximately caused the Data Breach which, in turn, directly and/or proximately resulted in the theft of Plaintiff's and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain for no permissible purpose under FCRA. St. Joseph's above-described willful and reckless FCRA violations also prevented it from timely and immediately notifying Plaintiff and Class Members about the Data Breach which, in turn, inflicted additional economic damages and other actual harm on them.

77. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute the willful and/or reckless violation of FCRA. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred, and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and

wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, (vii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date, and/or (viii) statutory damages of not less than \$100, and not more than \$1000, each.

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT (15 U.S.C. § 1681, *et seq.*)

78. The preceding factual statements and allegations are incorporated by reference.

79. In the alternative, by its above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—St. Joseph negligently and/or in a grossly negligent manner violated FCRA; to wit, St. Joseph negligently and/or in a grossly negligent manner

violated 15 U.S.C. § 1681(b), 15 U.S.C. § 1681a(d)(3), 15 U.S.C. § 1681b(a);(g), and/or 15 U.S.C. § 1681c(a)(6) (and the related applicable regulations) by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI which, in turn, directly and/or proximately caused the Data Breach which, in turn, directly and/or proximately resulted in the theft of Plaintiff's and Class Members' unencrypted PII/PHI and its wrongful dissemination into the public domain for no permissible purpose under FCRA. St. Joseph's above-described negligent and/or grossly negligent FCRA violations also prevented it from timely and immediately notifying Plaintiff and Class Members about the Data Breach which, in turn, inflicted additional economic damages and other actual harm on them.

80. It was reasonably foreseeable to St. Joseph that its failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI would result in a data breach whereby unauthorized third parties would gain access to, and disseminate, Plaintiff's and Class Members' PII/PHI into the public domain for no permissible purpose.

81. Plaintiff and Class Members, therefore, are entitled to compensation for their economic damages and other actual harm, including (i) actual identity

theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and/or (vii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT III

VIOLATION OF THE TEXAS MEDICAL PRACTICE ACT (TEX. OCC. CODE § 159.001, et seq.)

82. The previous factual statements and allegations are incorporated by reference.

83. Under TEX. OCC. CODE § 159.002(a);(b), communications between a physician and a patient, relative to, or in connection with, any professional services provided by a physician to a patient, including records of the identity, diagnosis, evaluation, or treatment of a patient by a physician that is created or maintained by a physician, are confidential and privileged.

84. Under TEX. OCC. CODE § 159.002(c), a person, including a hospital, that receives information from a confidential communication or record as described above and acts on the patient's behalf, may not disclose such information

except to the extent disclosure is consistent with the authorized purposes for which the information was first obtained.

85. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute the unauthorized release of confidential and privileged communications in violation of the Texas Medical Practice Act. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, under TEX. OCC. CODE § 159.009, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished

value of the medical services they purchased from St. Joseph, and/or (vii) emotional distress from the compromise of their PII/PHI, and/or the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT IV

VIOLATION OF THE TEXAS HOSPITAL LICENSING LAW (TEX. HEALTH & SAFETY CODE § 241.001, et seq.)

86. The previous factual statements and allegations are incorporated by reference.

87. Under TEX. HEALTH & SAFETY CODE § 241.151(2), “health care information” is any information, including payment information, recorded in any form or medium that identifies a patient and relates to the history, diagnosis, treatment, or prognosis of a patient.

88. Under TEX. HEALTH & SAFETY CODE § 241.152(a), except as authorized by TEX. HEALTH & SAFETY CODE § 241.153 (which does not apply here), a hospital or an agent or employee of a hospital may not disclose “health care information” about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.

89. Under TEX. HEALTH & SAFETY CODE § 241.155, a hospital shall adopt and implement reasonable safeguards for the security of all “health care information” it maintains.

90. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' "health care information" (*i.e.*, their PII/PHI)—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm and damages, and collectively constitute (i) the unauthorized disclosure of Plaintiff's and Class Members' "health care information" (*i.e.*, their PII/PHI) to unauthorized parties, and (ii) St. Joseph's failure to adopt and implement reasonable safeguards for the security of Plaintiff's and Class Members' PII/PHI entrusted to it—both of which are violations of the Texas Hospital Licensing Law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, under TEX. HEALTH & SAFETY CODE § 241.156, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of

their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and/or (vii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT V

NEGLIGENCE/GROSS NEGLIGENCE

91. The previous factual statements and allegations are incorporated by reference.

92. Upon coming into possession of Plaintiff's and Class Members' private, confidential, non-public, and sensitive PII/PHI, St. Joseph had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the PII/PHI from being stolen and compromised. St. Joseph's duty arises from Texas common law, in part, because it was reasonably foreseeable to St. Joseph under the circumstances that a data breach in its computer system was likely to occur that would cause Plaintiff and Class Members to suffer the above-described economic damages and other actual harm. St. Joseph's duty also arises from the PII/PHI security obligations expressly imposed upon it by, *inter alia*, HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas

Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed.” *See* Exhibit B at 3.

93. St. Joseph also had a duty to timely disclose the Data Breach to Plaintiff and Class Members so they could take the appropriate defensive steps necessary to minimize their economic damages and other actual harm. Instead, by its above-described wrongful actions, inaction and/or omissions, and delayed disclosure of the Data Breach, St. Joseph shifted its notification obligation and expenses to Plaintiff and Class Members. St. Joseph also (i) directly and/or proximately caused Plaintiff and Class Members to suffer the above-described economic damages and other actual harm, (ii) saved the cost of implementing the proper patient data security measures, policies, procedures, protocols, and software and hardware systems, and (iii) wrongfully shifted the risk and expense of the Data Breach to Plaintiff and Class Members. St. Joseph’s duty to properly and timely disclose the Data Breach to Plaintiff and Class Members also arises from the same above-described sources.

94. St. Joseph also had a duty to identify, implement, maintain and monitor the appropriate customer data security measures, policies, procedures, protocols, and software and hardware systems within its computer system and servers to prevent and detect data breaches and the unauthorized dissemination of Plaintiff’s and Class Members’ PII/PHI—including their PII/PHI stolen and

compromised by the Data Breach. Such duty also arises from the same above-described sources.

95. St. Joseph, by and through its above-described negligent and/or grossly negligent actions, inaction, and/or omissions, breached its duties to Plaintiff and Class Members by, *inter alia*, failing to identify, implement, maintain and monitor the appropriate data security measures, policies, procedures, protocols, and software and hardware systems within its computer system and servers, and failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' private, non-public, sensitive PII/PHI within St. Joseph's possession, custody and control.

96. St. Joseph, by and through its above-described negligent and/or grossly negligent actions, inaction, omissions and/or silence when it had a duty to speak, also breached its duties to Plaintiff and Class Members by failing to (i) advise Plaintiff and Class Members that the appropriate data security measures, policies, procedures, protocols, and software and hardware systems within its computer system and servers, in fact, were not in place, properly functioning and/or monitored, and (ii) timely notify them of the Data Breach so they could take the necessary defensive steps to minimize their economic damages and other actual harm. But for St. Joseph's grossly negligent, negligent and/or wrongful breach of the duties it owed (and continues to owe) Plaintiff and Class Members, their

private, confidential, non-public, sensitive PII/PHI would never have been stolen compromised, and disseminated to the world, the Data Breach would not have occurred, and Plaintiff and Class Members would not have suffered the economic damages and other actual harm they have suffered.

97. The Data Breach and the resulting economic damages and other actual harm suffered by Plaintiff and Class Members were reasonably foreseeable consequences of St. Joseph's negligence and/or gross negligence.

98. The economic loss doctrine does not apply to bar Plaintiff's and Class Members' negligence and/or gross negligence claims because, *inter alia*, (i) St. Joseph is in the business of supplying information for the guidance of Plaintiff and Class Members regarding their health care and/or securing payment from Plaintiff and Class Members for the provision of health care services, and (ii) St. Joseph made the above-described negligent and/or grossly negligent misrepresentations regarding the data security "tools" it had in place and/or engaged in the above-described negligent and/or grossly negligent conduct.

99. Adding to St. Joseph's negligence, gross negligence, and violations of HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to "meet or exceed" (*see* Privacy Notice (Exhibit B)

at 3) is the fact that St. Joseph was on notice that approximately 94% of all healthcare organizations in the United States have suffered data breaches in the last two (2) years.¹⁴ This is publicly available information St. Joseph knew, or should have known, that should have prompted St. Joseph to institute the appropriate data security measures, policies, procedures, protocols, and software and hardware systems within its computer system and servers to properly safeguard and protect Plaintiff's and Class Members' PII/PHI.

100. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute negligence and/or gross negligence at Texas common law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the

¹⁴ *Ponemon Study Reveals Ninety-Four Percent of Hospitals Surveyed Suffered Data Breaches* (Dec. 6, 2013), <http://www2.idexpertscorp.com/press/ninety-four-percent-of-hospitals-surveyed-suffered-data-breaches/> (last visited March 27, 2014).

world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT VI

NEGLIGENCE *PER SE*

101. The preceding statements and allegations are incorporated by reference.

102. At all relevant times, St. Joseph's was required (and continues to be required) to comply with, *inter alia*, HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to "meet or exceed" (*see* Privacy Notice (Exhibit B) at 3) requiring it to, *inter alia*, (i) identify, implement, maintain and monitor the appropriate data security measures, policies,

procedures, protocols, and software and hardware systems in its computer system and servers, (ii) safeguard, protect, and not disclose Plaintiff's and Class Members' PII/PHI within St. Joseph's possession, custody and control to unauthorized parties, and (iii) notify Plaintiff and Class Members about the Data Breach as quickly as possible. These statutes and standards establish the duty of care owed by St. Joseph to Plaintiff and Class Members.

103. By its above-described wrongful actions, inaction, omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—the resulting Data Breach, its failure to notify Plaintiff and Class Members such data security measures, policies, procedures, protocols, and software and hardware systems, in fact, were not in place, operational, and/or monitored, and its failure to timely notify Plaintiff and Class Members about the Data Breach, St. Joseph knowingly, and without excuse, violated HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed” (*see* Privacy Notice (Exhibit B) at 3). Had St. Joseph complied with such laws and standards during the relevant time period, the Data Breach would not

have occurred, and the resulting economic damages and other actual harm would not have been inflicted on Plaintiff and Class Members.

104. Plaintiff and Class Members are members of the class of persons intended to be protected by HIPAA, the Texas Medical Records Privacy Act, the Texas Medical Practice Act, the Texas Hospital Licensing Law, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed.” *See* Privacy Notice (Exhibit B) at 3. The above-described economic damages and other actual harm suffered by Plaintiff and Class Members as a direct and/or proximate result of the Data Breach—for which they are entitled to compensation—are the types of injuries and harm intended to be prevented by these laws and standards.

105. St. Joseph’s above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph’s failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff’s and Class Members’ PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff’s and Class Members’ PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute negligence *per se* at Texas common law. Had St.

Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, under TEX. OCC. CODE § 159.009, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) emotional distress from the compromise of their PII/PHI, and/or the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT VII

BREACH OF CONTRACT

106. The preceding factual statements and allegations are incorporated by reference.

107. Plaintiff and Class Members, on the one hand, and St. Joseph, on the other hand, mutually intended to form and, in fact, formed and entered into valid and enforceable contracts arising from, and evidenced by, the Privacy Notice (Exhibit B). Such contracts govern the Parties' business relationships.

108. Under the terms of such contracts, Plaintiff and Class Members promised to pay money to St. Joseph in exchange for health care services, including protection of their PII/PHI. St. Joseph's contractual obligation to safeguard and protect Plaintiff's and Class Members' PII/PHI is a material term of such contracts and continues in full force and effect.

109. All conditions precedent to St. Joseph's liability under these contracts have been performed by Plaintiff and Class Members. Plaintiff and Class Members performed all of their obligations under the contracts by paying St. Joseph for health care services and protection of their PII/PHI. St. Joseph, however, breached its contracts with Plaintiff and Class Members by knowingly, maliciously, fraudulently, willfully, wantonly, negligently and wrongfully failing to safeguard and protect their PII/PHI as described above.

110. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—breached its contracts with Plaintiff and Class Members and directly and/or proximately caused Plaintiff and Class Members to suffer economic damages and other actual harm in the form of, *inter alia*, the lost benefit of their bargains; to wit, Plaintiff and Class Members understood, agreed and expected that

a portion of the price they paid to St. Joseph for health care services would be spent by St. Joseph to safeguard and protect their PII/PHI—especially in light of St. Joseph’s representations in its Privacy Notice. Although Plaintiff and Class Members paid for the protection of their PII/PHI, St. Joseph failed to do so, thereby resulting in its theft and dissemination to the world and Plaintiff’s and Class Members’ lost benefit of their bargains. St. Joseph’s above-described wrongful actions, inaction and/or omissions and the resulting Data breach constitute breach of contract at Texas common law—for which Plaintiff and Class Members are entitled to recover the lost benefit of their bargains.

COUNT VIII

BREACH OF IMPLIED CONTRACT

111. The preceding factual statements and allegations are incorporated by reference.

112. In the alternative, Plaintiff and Class Members, on the one hand, and St. Joseph, on the other hand, mutually intended to form and, in fact, formed and entered into valid and enforceable implied contracts arising from, and evidenced by, the Parties’ acts and conduct and the Privacy Notice (Exhibit B). Such implied contracts govern the Parties’ business relationships, and consist of obligations arising from their mutual agreement and intent to promise where such agreements and promises are not specifically expressed in words in other agreements, if any.

113. Under the terms of such implied contracts, Plaintiff and Class Members promised to pay money to St. Joseph in exchange for health care services, including protection of their PII/PHI. St. Joseph's contractual obligation to safeguard and protect Plaintiff's and Class Members' PII/PHI is a material term of such implied contracts and continues in full force and effect.

114. All conditions precedent to St. Joseph's liability under these implied contracts have been performed by Plaintiff and Class Members. Plaintiff and Class Members performed all of their obligations under the implied contracts by paying St. Joseph for health care services and protection of their PII/PHI. St. Joseph, however, breached its implied contracts with Plaintiff and Class Members by knowingly, maliciously, fraudulently, willfully, wantonly, negligently and wrongfully failing to safeguard and protect their PII/PHI as set forth above.

115. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—breached its implied contracts with Plaintiff and Class Members and directly and/or proximately caused them to suffer economic damages and other actual harm in the form of, *inter alia*, the lost benefit of their bargains; to wit, they understood, agreed and expected that a portion of the price they paid to

St. Joseph for health care services would be spent by St. Joseph to safeguard and protect their PII/PHI—especially in light of St. Joseph’s representations in its Privacy Notice. Although Plaintiff and Class Members paid for protection of their PII/PHI, St. Joseph failed to do so, thereby resulting in its theft and dissemination to the world and Plaintiff’s and Class Members’ lost benefit of their bargains. St. Joseph’s above-described wrongful actions, inaction and/or omissions constitute breach of implied contract at Texas common law—for which Plaintiff and Class Members are entitled to recover the lost benefit of their bargains.

COUNT IX

VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES-CONSUMER PROTECTION ACT

116. The preceding factual statements and allegations are incorporated by reference.

117. Plaintiff and Class Members are “consumers” under the Texas Deceptive Trade Practices-Consumer Protection Act (“DTPA”), under Section 17.45(4) of the Texas Business and Commerce Code, by purchasing health care services and PII/PHI protection services from St. Joseph. St. Joseph is a “person” that may be sued under the DTPA, under Section 17.45(3) of the Texas Business and Commerce Code, for providing such services.

118. By its above-described unconscionable actions and/or unconscionable course of action, inaction and/or omissions and the resulting Data Breach, St.

Joseph knowingly and intentionally violated Section 17.50(a)(3) of the Texas Business and Commerce Code by failing to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—while, at the same time, falsely representing in its Privacy Notice that such data security measures, policies, procedures, protocols, and software and hardware systems were in place, operational and/or monitored (which they were not) (in violation of Section 17.46(b)(5); (b)(7) of the Texas Business and Commerce Code)—which, as a direct and/or proximate result, was disclosed, stolen, compromised and disseminated to the world in the Data Breach.

119. St. Joseph's above-described wrongful actions, inaction and/or omissions and the resulting Data Breach unfairly took advantage of the lack of knowledge, ability, and experience of Plaintiff and Class Members to a grossly unfair degree regarding St. Joseph's computer system and servers and St. Joseph's inability to safeguard and protect their PII/PHI; to wit, at the time Plaintiff and Class Members gave St. Joseph their PII/PHI in connection with purchasing health care services, Plaintiff and Class Members did not know, and had no way of knowing, nor did St. Joseph disclose, that it was incapable of safeguarding and protecting their PII/PHI. In fact, the opposite occurred; St. Joseph falsely represented in its Privacy Notice (Exhibit B) (in violation of Section 17.46(b)(5);

(b)(7) of the Texas Business and Commerce Code) that it had data security measures, policies, procedures, protocols, and software and hardware systems in place to safeguard and protect Plaintiff's and Class Members' PII/PHI—which admittedly turned out not to be the case. *See* Exhibit A.

120. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, and caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute violations of Section 17.50(a)(3) of the Texas Business and Commerce Code (as well as Section 17.46(b)(5); (b)(7) of the Texas Business and Commerce Code). Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, under Section 17.50 of the Texas Business and Commerce Code, including (i) actual identity theft, identity fraud and/or medical

fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) emotional distress from the compromise of their PII/PHI, and/or the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT X

INVASION OF PRIVACY

121. The preceding factual statements and allegations are incorporated by reference.

122. St. Joseph's intentional failure to safeguard and protect Plaintiff's and Class Members' PII/PHI directly and/or proximately resulted in an invasion of privacy by public disclosure of such highly confidential and private information.

123. Access to Plaintiff's and Class Members' PII/PHI, and the wrongful dissemination of such information into the public domain, was easily achieved because their PII/PHI (i) was not properly safeguarded and protected within St. Joseph's computer systems, (ii) easily accessed by data thieves via the Internet, and, (iii) on information and belief, easily accessed, bought, sold, disseminated and utilized without authorization after the theft because the information was either encrypted improperly or not encrypted at all.

124. St. Joseph's above-described wrongful dissemination of Plaintiff's and Class Members' PII/PHI into the public domain is not of a legitimate public concern; publicity of Plaintiff's and Class Members' PII/PHI would be, is and will continue to be offensive to Plaintiff, Class Members, and other reasonable people.

125. St. Joseph intentionally invaded Plaintiff's and Class Members' privacy by disseminating their PII/PHI to the world by repeatedly failing and refusing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the security and confidentiality of their PII/PHI.

126. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure and dissemination to the world of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute an invasion of Plaintiff's and Class Members' privacy at Texas common law by publicly disclosing their private facts (*i.e.*, their PII/PHI). Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would

have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) emotional distress from the compromise of their PII/PHI, and/or the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT XI

BREACH OF FIDUCIARY DUTY

127. The preceding factual statements and allegations are incorporated by reference.

128. As demonstrated by TEX. OCC. CODE § 159.002(a);(b), communications between a physician and a patient, relative to or in connection with any professional services provided by a physician to a patient, including records of the identity, diagnosis, evaluation, or treatment of a patient by a

physician created or maintained by a physician—such as Plaintiff’s and Class Members’ PII/PHI—are confidential and privileged.

129. As further demonstrated by TEX. OCC. CODE § 159.002(c), a person, including a hospital, that receives information from a confidential communication or record as described above, and acts on the patient's behalf, may not disclose such information except to the extent the disclosure is consistent with the authorized purposes for which the information was first obtained.

130. As further demonstrated by TEX. HEALTH & SAFETY CODE § 241.151(2), “health care information” is any information, including payment information, recorded in any form or medium, that identifies a patient and relates to the history, diagnosis, treatment, or prognosis of a patient—such as Plaintiff’s and Class Members’ PII/PHI.

131. As further demonstrated by TEX. HEALTH & SAFETY CODE § 241.152(a), except as authorized by TEX. HEALTH & SAFETY CODE § 241.153 (which does not apply here), a hospital or an agent or employee of a hospital may not disclose “health care information” about a patient—such as Plaintiff’s and Class Members’ PII/PHI—to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.

132. The unique, personal, private, and highly confidential nature of PII/PHI itself, including the PII/PHI entrusted by Plaintiff and Class Members to St. Joseph, and the absolute duty to safeguard and protect PII/PHI imposed on St. Joseph by the above statutes, as well as HIPAA, Sections 521.052 and 521.053 of the Texas Business and Commerce Code, and/or the industry standards referenced in its Privacy Notice that it claims to “meet or exceed” (*see* Exhibit B at 3), confirm that St. Joseph was (and continues to be) in personal, confidential and fiduciary relationships with Plaintiff and Class Members as a matter of Texas law.

133. As fiduciaries, St. Joseph owed (and continues to owe) Plaintiff and Class Members (i) the commitment to deal fairly and honestly, (ii) the duties of good faith and undivided loyalty, and (iii) integrity of the strictest kind. St. Joseph was (and continues to be) obligated to exercise the highest degree of care in carrying out its obligations to Plaintiff and Class Members under the Parties’ confidential, special and fiduciary relationships including, without limitation, safeguarding and protecting Plaintiff’s and Class Members’ PII/PHI.

134. St. Joseph breached its fiduciary duties to Plaintiff and Class Members by failing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiff’s and Class Members’ PII/PHI which, in turn, directly and/or proximately caused the Data

Breach, and the theft, compromise, dissemination to the world, and wrongful use of their PII/PHI, as described above. St. Joseph also breached its fiduciary duties to Plaintiff and Class Members by failing to failing to (i) advise Plaintiff and Class Members that the appropriate data security measures, policies, procedures, protocols, and software and hardware systems within its computer system and servers, in fact, were not in place, properly functioning and/or monitored (but misrepresenting the exact opposite in the Privacy Notice), and (ii) timely notify them of the Data Breach so they could take the necessary defensive steps to minimize their economic damages and other actual harm.

135. To the extent either of the Defendants is a fiduciary that did not breach its fiduciary duties to Plaintiff and Class members, such Defendant is nonetheless liable because it had knowledge of the breaches of fiduciary duties committed by the other fiduciary, and did not make reasonable efforts under the circumstances to prevent and/or remedy such fiduciary breaches.

136. St. Joseph willfully and wantonly breached its fiduciary duties to Plaintiff and Class Members or, at the very least, committed these breaches with conscious indifference and reckless disregard of their rights and interests.

137. St. Joseph's above-described wrongful actions, inaction and/or omissions directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, caused

Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute breach of fiduciary duty at Texas common law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) emotional distress from the compromise of their PII/PHI, and/or the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT XII

BREACH OF CONFIDENTIALITY

138. The preceding factual statements and allegations are incorporated by reference.

139. Plaintiff's and Class Members' unique, personal, and private PII/PHI delivered to St. Joseph for safekeeping was (and continues to be) highly confidential.

140. St. Joseph breached the confidentiality of Plaintiff's and Class Members' PII/PHI by failing to identify, implement, maintain and/or monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems to ensure the security and confidentiality of Plaintiff's and Class Members' PII/PHI which, in turn, directly and/or proximately caused the Data Breach, and the theft, compromise, dissemination to the world, and wrongful use of their PII/PHI, as described above.

141. St. Joseph's above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—directly and/or proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiff's and Class Members' PII/PHI, caused Plaintiff and Class Members to suffer economic damages and other actual harm, and collectively constitute breach of confidentiality at Texas common law. Had St. Joseph not engaged in such wrongful actions, inaction and/or omissions, the Data Breach never would have occurred and Plaintiff's and Class Members' PII/PHI

would not have been stolen, compromised, disseminated to the world, and wrongfully used. Plaintiff and Class Members, therefore, are entitled to injunctive relief and/or compensation for their economic damages and other actual harm, including (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) lost benefit of their bargains, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vi) diminished value of the medical services they purchased from St. Joseph, and (vii) emotional distress from the compromise of their PII/PHI, and/or the resulting identity theft, identity fraud and/or medical fraud experienced to date.

COUNT XIII

MONEY HAD AND RECEIVED/ASSUMPSIT

142. The preceding factual statements and allegations are incorporated by reference.

143. Plaintiff pleads this Count in the alternative to its breach of contract claims because Plaintiff and Class Members cannot recover under this Count and under their breach of contract counts.

144. By its above-described wrongful actions, inaction and/or omissions—to wit, St. Joseph's failure to identify, implement, maintain and monitor the proper data security measures, policies, procedures, protocols, and software and hardware

systems to safeguard and protect Plaintiff's and Class Members' PII/PHI—and the resulting Data Breach, St. Joseph holds money conferred on it by Plaintiff and Class Members—*i.e.*, that portion of the health services purchase prices Plaintiff and Class Members paid St. Joseph for protecting their PII/PHI, which St. Joseph admittedly failed to do. *See* Exhibit A. St. Joseph has been unjustly enriched by the funds it should have spent to safeguard and protect their PII/PHI which, in equity and good conscience, belongs to Plaintiff and Class Members, and should be refunded, because St. Joseph failed to do so.

145. St. Joseph also continues to be unjustly enriched by, *inter alia*, (i) the saved cost of implementing the proper PII/PHI security measures, policies, procedures, protocols, and software and hardware systems in its computer system and servers, which it did not implement, (ii) the shifted risk and expense of the Data Breach to Plaintiff and Class Members, and (iii) the return on investment on all above-described amounts.

146. St. Joseph, therefore, should be compelled to refund (or disgorge) such wrongfully collected, saved back and/or shifted funds and expenses under the common law equitable doctrine of money had and received and/or the duty to make restitution under the common law equitable doctrine of assumpsit.

RELIEF REQUESTED

147. The preceding factual statements and allegations are incorporated by reference.

148. **ACTUAL, CONSEQUENTIAL DAMAGES AND/OR NOMINAL DAMAGES.**

As a direct and/or proximate result of St. Joseph's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and Class Members have suffered (and continue to suffer) economic damages and other actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud and/or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under FCRA, (v) lost benefit of their bargains, (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vii) diminished value of the medical services they purchased from St. Joseph, and (viii) emotional distress from the compromise of their PII/PHI, and the resulting identity theft, identity fraud and/or medical fraud experienced to date—for which they are entitled to compensation. Plaintiff's and Class Members' damages were foreseeable by St. Joseph and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

149. **EXEMPLARY DAMAGES.** Plaintiff and Class Members also are entitled to exemplary damages as punishment and to deter such wrongful actions, inaction

and/or omissions in the future. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

150. **DTPA TREBLE DAMAGES.** Plaintiff and Class Members are also entitled to treble damages for St. Joseph's knowing, willful, intentional, wrongful and unconscionable conduct in violation of Section 17.50(a)(3) of the Texas Business and Commerce Code, under Section 17.50(b)(1) of the Texas Business and Commerce Code. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

151. **INJUNCTIVE RELIEF.** Plaintiff and Class Members also are entitled to injunctive relief requiring St. Joseph to, *inter alia*, (i) immediately disclose to Plaintiff and Class Members the precise nature, breadth, scope and extent of their stolen and compromised PII/PHI, including the specific information comprising the stolen "medical information," (ii) make prompt and detailed disclosure to all past, present and future patients affected by any future data breaches of their PII/PHI, (iii) immediately encrypt the PII/PHI of its past, present, and future patients within its possession, custody and control, (iv) implement the above-referenced proactive policies and procedures in order to secure and protect its patients' PII/PHI and be in a position to immediately notify them about any data breaches, (v) submit to periodic compliance audits by a third party regarding the implementation of and compliance with such policies and procedures, and (vi)

submit to periodic compliance audits by a third party regarding the security of its patients' PII/PHI within its possession, custody and control. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

152. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiff and Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia*, (i) 15 U.S.C. §§ 1681n(a); o(a), (ii) Chapter 38 of the Texas Civil Practice and remedies Code, and (iii) Section 17.50(d) of the Texas Business and Commerce Code. All conditions precedent to Plaintiff's and Class Members' claims for relief have been performed and/or occurred.

WHEREFORE, Plaintiff, on behalf of herself and Class Members, respectfully requests that (i) St. Joseph be cited to appear and answer this lawsuit, (ii) this action be certified as a class action, (iii) Plaintiff be designated the Class Representative, and (iv) Plaintiff's counsel be appointed Class Counsel. Plaintiff, on behalf of herself and Class Members, further requests that upon final trial or hearing, judgment be awarded against St. Joseph, in favor of Plaintiff and the Class Members, for:

- (i) actual damages, consequential damages. nominal damages, and/or FCRA statutory damages (as described above) in an amount to be determined by the trier of fact;

- (ii) exemplary damages;
- (iii) treble damages as set forth above;
- (iv) injunctive relief as set forth above;
- (v) pre- and post-judgment interest at the highest applicable legal rates;
- (vi) attorneys' fees and litigation expenses incurred through trial and any appeals;
- (vii) costs of suit; and
- (viii) such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of herself and all others similarly situated, respectfully demands a trial by jury on all of her claims and causes of action so triable.

Date: June 30, 2014

Respectfully submitted,

/s/ Richard L. Coffman

Richard L. Coffman

THE COFFMAN LAW FIRM

505 Orleans St., Ste. 505

Beaumont, TX 77701

Telephone: (409) 833-7700

Facsimile: (866) 835-8250

Email: rcoffman@coffmanlawfirm.com

Mitchell A. Toups

WELLER, GREEN, TOUPS & TERRELL, LLP

2615 Calder Ave., Suite 400

Beaumont, TX 77702

Telephone: (409) 838-0101

Facsimile: (409) 838-6780

Email: matoups@wgttlaw.com

Jason Webster
THE WEBSTER LAW FIRM
6200 Savoy, Suite 515
Houston, TX 77036
Telephone: (713) 581-3900
Facsimile: (713) 409-6464
Email: jwebster@thewebsterlawfirm.com

CERTIFICATE OF SERVICE

I certify that a true and correct copy of Plaintiff's First Amended Class Action Complaint was served on the following counsel of record, via the Court's ECF System, on June 30, 2014.

/s/ Richard L. Coffman
Richard L. Coffman

Kent Adams
Kristie Johnson
LEWIS BRISBOIS BISGAARD & SMITH, LLP
Weslayan Tower, Suite 1400
24 East Greenway Plaza
Houston, Texas 77046
Telephone: (713) 659-6767
Facsimile: (713) 759-6830
Email: Kent.adams@lewisbrisbois.com
Email: Kristie.johnson@lewisbrisbois.com

ATTORNEYS FOR DEFENDANTS